Counterfeit, Fraudulent and Suspect Parts

Industry Perspective

NRC Public Meeting June 30, 2011

Mark Harvey
mwh@nei.org

NUCLEAR ENERGY INSTITUTE

Agenda

- Definitions
- Applicability
- Historical Performance
- Preventive Measures
- Procurement
- Maintenance
- Corrective Action
- NUPIC
- EPRI
- Cyber Security

Definition

- Counterfeit, Fraudulent, and Suspect Items
  - Counterfeit - Intentionally manufactured or altered to imitate a legitimate product without the legal right to do so
  - A counterfeit item is one that has been fabricated in imitation of something else with purpose to defraud by passing the false copy for genuine or original or is an item copied without the legal right or authority to do so

Definition

- Fraudulent - Items that are intentionally misrepresented with intent to deceive. Fraudulent items include items provided with incorrect identification or falsified or inadequate certification.

- Suspect - Items that are suspected of being counterfeit, fraudulent, or substandard

Applicability

- XV. Nonconforming Materials, Parts, or Components

  Measures shall be established to control materials, parts, or components *which do not conform to requirements* in order to prevent their inadvertent use or installation.

  These measures shall include, as appropriate, procedures for identification, documentation, segregation, disposition, and notification to affected organizations.

Applicability

- XVI. Corrective Action

  Measures shall be established to assure that conditions adverse to quality, such as failures, malfunctions, deficiencies, deviations, defective material and equipment, and nonconformances are promptly identified and corrected. In the case of significant conditions adverse to quality, the measures shall assure that the cause of the condition is determined and corrective action taken to preclude repetition.

  * - Failure to meet technical requirements is a nonconforming material condition requiring resolution and reportability evaluation

  * - Nonconformance and Corrective Action Programs identify failure to comply with requirements. Causal determination would identify CSFI if warranted.

Applicability

- Nuclear Industry minimally impacted due to characteristics of design:
  - Failures not repeatable and large numbers
  - Procurement from Original Equipment Manufacturer whenever possible
  - Receipt Inspection Process
  - Equivalency evaluations when item not available
  - Limited opportunity for CFSI
- While limiting opportunity, processes must remain robust to prevent introduction

Historical Performance

- EPRI Database of CFSI indicates reporting of issues when appropriate:
  - 7/6/2010 – 1.5” non-safety related gate valve caught during receipt inspection (Diablo Canyon)
  - 9/1/2009 – Non-safety related optocouplers caught during receipt inspection (Amidyne Group)
  - Others listed in EPRI Presentation

Preventive Measures

- Preventive measures focus on safety related items
  - Counterfeit, Fraudulent, and Suspect Parts = Departure from technical requirements of a purchase order
  - Reportability under Part 21, Part 50.55(e) and Part 72, 73 for Significant Safety Hazards caused by CSFI
  - Industry focus on identification of nonconforming items – CFSI is a subset
  - Corrective Action Programs used to evaluate impact and extent of condition, and ensure notification and action

Procurement

- Development of standard Procurement Clause wording in purchasing documents
  - Extended to non-safety related
- Supplier training at industry meetings
- CFSI focus of Industry Procurement support groups

Maintenance

- Maintenance practices require “like for like” validation
- Training provided to maintenance personnel

Corrective Action Programs

- Requires identification, correction, and documentation
- Adverse conditions identified in Corrective Action Programs
- “Significant Conditions” require root cause evaluation – Identify CFSI if appropriate
- Lower significance CFSI identified through Apparent Cause evaluation of adverse trend

Corrective Action Programs

- Significant conditions and adverse trends identified through CAP designated as non-CAQ, but same process used
- Program includes ties to NRC notification through 10CFR21 notification for issues affecting or potentially affecting safety related SSCs

NUPIC

- 2008 – EPRI Training provided to NUPIC Auditors
- 2009 - NUPIC Checklist modified to include controls for prevention of CFSI
- 2009 - Routine interaction with NRC and EPRI regarding tools to prevent introduction of CFSI
- Robust supplier finding process
- Industry Issues shared through NUPIC Database, Notification Processes, and NUPIC Meetings

NUPIC Checklist Revision

Assess and describe inspection/testing processes, such as receipt, in-process, and final inspection or testing, for identifying CSFI:

- Altered manufacturer's name, logo, serial number, manufacturing date
- Items differing in configuration, dimensions, fit, finish, color, or other attributes from that expected
- Markings on items or documentation are missing, unusual, altered, or inconsistent with that expected
- Markings or documentation from country other than the subsupplier
- Items, sold as new, exhibit evidence of prior use
- Performance inconsistent with specifications, certification or test data
- Documentation that appear altered, incomplete, or lack expected traceability, UL or manufacturer's markings

* - For CSFI identified during customer Receipt Inspection, the Supplier is responsible for performing 10CFR21 evaluation

EPRI Interaction

- Potential CFSI communicated to EPRI and included in industry database
- Notifications made to users based on standard equipment lists
- Established group to monitor and communicate

Cyber Security

- 10 CFR 73.54(a)(1) requires licensees to protect digital computer and communications systems and networks associated with the following categories of functions, from those cyber attacks in 10 CFR 73.54(a)(2):
  - Safety-related and important-to-safety functions
  - Security functions
  - Emergency Preparedness (EP) functions, including offsite communications
  - Support systems and equipment which, if compromised, would adversely impact safety, security, or EP functions

Cyber Security

- Cyber Security Program establishes defense-in-depth capabilities to detect, respond to, and recover from cyber attacks
  - Equipment under the CSP include those associated with safety, important to safety, security, and emergency preparedness including offsite communications, and their support systems
  - Protected equipment are Critical Digital Assets

Cyber Security

- Defense in Depth
  - In the event failure in prevention were to occur (policy violation) or protection mechanisms were bypassed (new virus that is not yet identified as a cyber attack)
  - Mechanisms remain in place to:
    - Detect and respond to an unauthorized alteration in an impacted CDA
    - Mitigate the impacts of this alteration
    - Recover normal operations of the impacted CDA before an adverse impact

Cyber Security

- This operational program addresses threats by instituting cyber security controls.
- These controls include provisions for "System and Services Acquisition"
  - System and Services Acquisition Policy and Procedures
  - Supply Chain Protection
  - Trustworthiness
  - Integration of Security Capabilities
  - Developer Security Testing
  - Evaluation and Management of Cyber Risks

Cyber Security

- This operational program further enhances the industries existing efforts to threats associated address CFSI
- Cyber Security Programs will be implemented in accordance with an NRC approved implementation schedule

Summary

- Nuclear Plant CFSI Limited Susceptibility:
  - Robust QA requirements on suppliers
  - Reliance on OEMs and Qualified Suppliers
  - Effective Supplier Assessment process
  - Items not “Low Dollar – High Failure”
- Industry initiatives in place (NUPIC, EPRI) to protect against CFSI introduction
- Plant processes, such as Maintenance and Procurement, add layers of protection
- Industry prepared to work with NRC to enhance existing protections, as needed